UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/574,909 | 04/06/2006 | Vincent Carlier | 4005-0277PUS1 | 7126 |

77032 7590 01/24/2012

Joe McKinney Muncy
4000 Legato Raod, Suite 310
Fairfax, VA 22033

| EXAMINER | |
|---|---|
| LAFORGIA, CHRISTIAN A | |
| ART UNIT | PAPER NUMBER |
| 2439 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/24/2012 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* VINCENT CARLIER, HERVE CHABANNE,
and
EMMANUELLE DOTTAX

---

Appeal 2010-006646
Application 10/574,909
Technology Center 2400

---

Before DEBRA K. STEPHENS, DENISE M. POTHIER, and
BRUCE R. WINSOR, *Administrative Patent Judges*.

POTHIER, *Administrative Patent Judge*.

DECISION ON APPEAL

## STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-10. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

### *Invention*

Appellants' invention relates to a technique for protecting a cryptographic algorithm. *See generally* Spec. 1:2-3. Claim 1 is reproduced below with the key disputed limitation emphasized:

> 1. A method of *protecting a cryptographic algorithm (6) before introduction in an enciphering device* (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials ($P_i$) of at least two variables each, and having a degree of not less than two, the method comprising:
>
> providing to the enciphering device at least two initial polynomials ($P_i$, $P_{i+1}$);
>
> combining, on the enciphering device, combined polynomials ($Q_k$), each obtained from the at least two initial polynomials ($P_i$, $P_{i+1}$); and
>
> implementing the combined polynomials ($Q_k$) in the programmable processor unit (4).

The Examiner relies on the following as evidence of unpatentability:

| | | |
|---|---|---|
| Rajasekaran | US 4,922,539 | May 1, 1990 |
| Schwan | US 2004/0187035 A1 | Sept. 23, 2004 |

Bruce Schneier, *Applied Cryptography – Protocols, Algorithms, and Source Code in C* 270-285 (1996) ("Schneier").

## THE REJECTIONS

1. Claims 1-4 and 6-9 are rejected under 35 U.S.C. § 103(a) as unpatentable over Schwann, Rajasekaran, and Official Notice.[1] Ans. 3-5.[2]

2. Claims 5 and 10 are rejected under 35 U.S.C. § 103(a) as unpatentable over Schwann, Rajasekaran, Official Notice, and Schneier. Ans. 5.

## THE OBVIOUSNESS REJECTION OVER SCHWAN, RAJASEKARAN, AND OFFICIAL NOTICE

Regarding representative claim 1, the Examiner finds that factoring polynomials into quadratics and recombining polynomials is a well-known technique, as demonstrated by Rajasekaran and high school algebra skills, regardless of its use. Ans. 3, 7. The Examiner concludes that combining this known practice with Schwan's cryptographic algorithm to protect the algorithm before its introduction into an enciphering device involves only routine skill in the art and yields a predictable result. Ans. 4.

Appellants argue that Schwan and Rajasekaran fail to teach or suggest protecting a cryptographic algorithm before introduction in a device. Br. 7. Also, Appellants assert that "[w]hile polynomial factoring algorithms may be used in the field of cryptology, their use is not inherent . . . in 'protecting a cryptographic algorithm before introduction in a device' as set forth in claim 1." Br. 8.

---

[1] The Examiner states "known techniques" but is taking Official Notice that factoring polynomial into quadratics and recombining them is common knowledge to ordinary skilled artisans. *See* Ans. 3.

[2] Throughout this opinion, we refer to the Appeal Brief filed October 9, 2009 and the Examiner's Answer mailed January 5, 2010.

## ISSUE

Under § 103, has the Examiner erred in rejecting claim 1 by finding that Schwan, Rajasekaran, and Official Notice collectively would have taught or suggested a method of protecting a cryptographic algorithm before introduction in an enciphering device (hereafter "limitation [1]")?

## ANALYSIS

We begin by construing the key disputed limitation of claim 1 or limitation [1]. As the Examiner states (Ans. 6), this disputed limitation is in the preamble and is not limiting because it only states the invention's purpose or intended use, and this preamble is not necessary to give life and meaning to the claim. *See American Medical Systems, Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358-59 (Fed. Cir. 2010). As a result, the discussed prior art (i.e., Schwan, Rajasekaran, and known techniques) do not have to teach this limitation. *See id.* at 1477. Appellants' contentions related to the prior art failing to teach protecting a cryptographic algorithm before introduction in an enciphering device (Br. 7-8) accordingly are not persuasive. *See In re Schreiber*, 128 F.3d 1473, 1476 (Fed. Cir. 1997).

Even assuming that the preamble is given patentable weight, we agree with the Examiner that this limitation is at best an intended use recitation, requiring the cited prior art as combined only to have the ability of performing limitation [1]. *See* Ans. 6. We look to Appellants' disclosure for an understanding of how a cryptographic algorithm is protected or how limitation [1] is performed. Appellants map limitation [1] to page 2, lines five through nine of the Specification (*see* Br. 4), which fails to provide any details about how the algorithm is protected (*see* Spec. 2:5-9). Appellants

further state that the invention's object (i.e., protecting the algorithm) is achieved through an algorithm transformation by forming initial polynomials, combining the combined polynomials, each obtained from at least two initial polynomials, and implementing the combined polynomials in the processor unit. Spec. 2:11-26. Thus, according to Appellants, a cryptographic algorithm is protected before introduction in an enciphering device[3] by performing the steps of transforming an algorithm to polynomials, combining the polynomials, and implementing the combined polynomials in a processor unit protects

Citing to Rajasekaran and known high school algebra techniques, the Examiner finds that factoring a polynomial such that at least two initial polynomials are provided and combining the combined polynomials, each obtained from the initial polynomials, is well-known. Ans. 3-4. Appellants do not challenge that these teachings are well-known to an ordinary skilled artisan (*see* Br. 7-8), and we adopt these findings and conclusions by the Examiner. In fact, Appellants also state that "polynomial factoring algorithms may be used in the field of cryptology." Br. 8. In other words, the Examiner's findings and Appellants' statement suggests that, polynomial factoring of cryptographic algorithms, including Schwan's taught

[3] Notably, the recitation in the preamble that recites "protecting a cryptographic algorithm [] *before* introduction in an enciphering device," (emphasis added) contrasts with the body of the claim that recites providing the polynomials *to the enciphering device*, combining the polynomials *on the enciphering device*, and implementing the combined polynomials *in* the enciphering device's *processor unit*. Similarly, independent claim 6 recites "[a]n enciphering device which utilizes a cryptographic algorithm" but the body of the claim recites "wherein the cryptographic algorithm is protected prior to its introduction into the enciphering device[.]"

cryptographic algorithms, is known by skilled artisans. Thus, the Examiner proposal of combining the discussed known techniques with the Schwan's cryptographic algorithm and device, such that the algorithm is implemented into Schwan's enciphering device's processing unit as the combined polynomials (Ans. 4), predictably yields no more than an ordinary skilled artisan would expect – protecting a cryptographic algorithm before its introduction into an enciphering device.

Appellants dispute the Examiner's statement in the Final Rejection that the claimed security features are inherent in factoring a cryptographic equation. *See* Br. 8. While the Examiner states that new uses inherently present in the prior art do not necessarily make claim 1 patentable (*see* Ans. 3, 7), the Examiner additionally relies on known techniques, as stated above, combined with Schwan's device to teach or suggest a method that has the ability to perform the function of limitation [1] recited in the preamble.

Lastly, merely pointing out what claim 1 recites and then asserting that the cited prior art fails to teach recited limitation (*see* App. Br. 7 stating neither Schwan nor Rajasekaran teaches or suggests the providing and implementing steps) is not considered a separate argument for patentability. *See In re Lovin*, 99 USPQ2d 1373, 1378-79 (Fed. Cir. 2011)

Based on the arguments presented, Appellants have not persuaded us of error in the rejection of independent claim 1 and claims 2, 4, 6, 7, and 9 not separately argued with particularity (Br. 7-9).

*Claims 3 and 8*

Regarding representative claim 3, the Examiner finds Schwan's teaching of erasing an algorithm from the computing device after the

housing is opened maps to an eraser member serving to erase both the processor unit and memory when an intrusion into the device occurs. Ans. 4, 9. Appellants argue that Schwan and Rajasekaran fail to teach or suggest an eraser member serving to erase the processor unit in the event of an intrusion into the device. Br. 9.

## ISSUE

Under § 103, has the Examiner erred in rejecting claim 3 by finding that Schwan, Rajasekaran, and Official Notice collectively would have taught or suggested an eraser member serving to erase the processor unit and memory in the event an intrusion into the device?

## ANALYSIS

Based on the record before us, we find no error in the Examiner's rejection. Schwan teaches the memory areas containing a secret check word, a secret key, and an secret encryption algorithm are erased if the housing is opened (e.g., an intrusion). *See* Schwan, ¶ 0013. Thus, Schwan's teaching cited by the Examiner (Ans. 4) is not limited to a single memory but includes memory *areas* that contain various information (e.g., secret check word, a secret key, an encryption algorithm). *See id.* Based on Schwan's teaching, an ordinary skilled artisan would have recognized that this information will be contained in various memory areas when the housing is opened and suggests erasing information from any or all memory areas, including memory associated with or within a programmable processing unit. We therefore disagree with Appellants that Schwan fails to teach or suggest an eraser member serving to erase the processor unit, as broadly as

recited, in the event an intrusion into the device as recited in claim 3. For the foregoing reasons, Appellants have not persuaded us of error in the rejection of claim 3 and claim 8 not separately argued with particularity (Br. 9).

THE OBVIOUSNESS REJECTION OVER SCHWAN, RAJASEKARAN, OFFICIAL NOTICE, AND SCHNEIER

Regarding claims 5 and 10, Appellants assert that Schneier fails to cure the purported deficiencies of claims 1 and 6. Br. 10. We are not persuaded for the reasons disclosed above when addressing claim 1 and need not address whether Schneier cures any alleged deficiency.

CONCLUSION

The Examiner did not err in rejecting claims 1-10 under § 103.

DECISION

The Examiner's decision rejecting claims 1-10 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

kis